University of Windsor

Faculty of Engineering
Department of Electrical and Computer Engineering

Intranets, Extranets, and Virtual Private Networks (VPNs)

S. Erfani
Summer 2003

Course Web site:

http://web4.uwindsor.ca/users/e/erfani/main.nsf

Outline

- Intranets and their applications
- Extranets and their applications
- Firewalls
- The Virtual Private Networks (VPN) concept and its objectives
- Types of VPNs
- Applications of Internet-Based VPNs
- Tunneling techniques for Internet-based VPNs
- IP Security

- References:
  - Chapter 16, pp. 482-517 of Text
  - Chapter 20, pp. 616-634 of Text

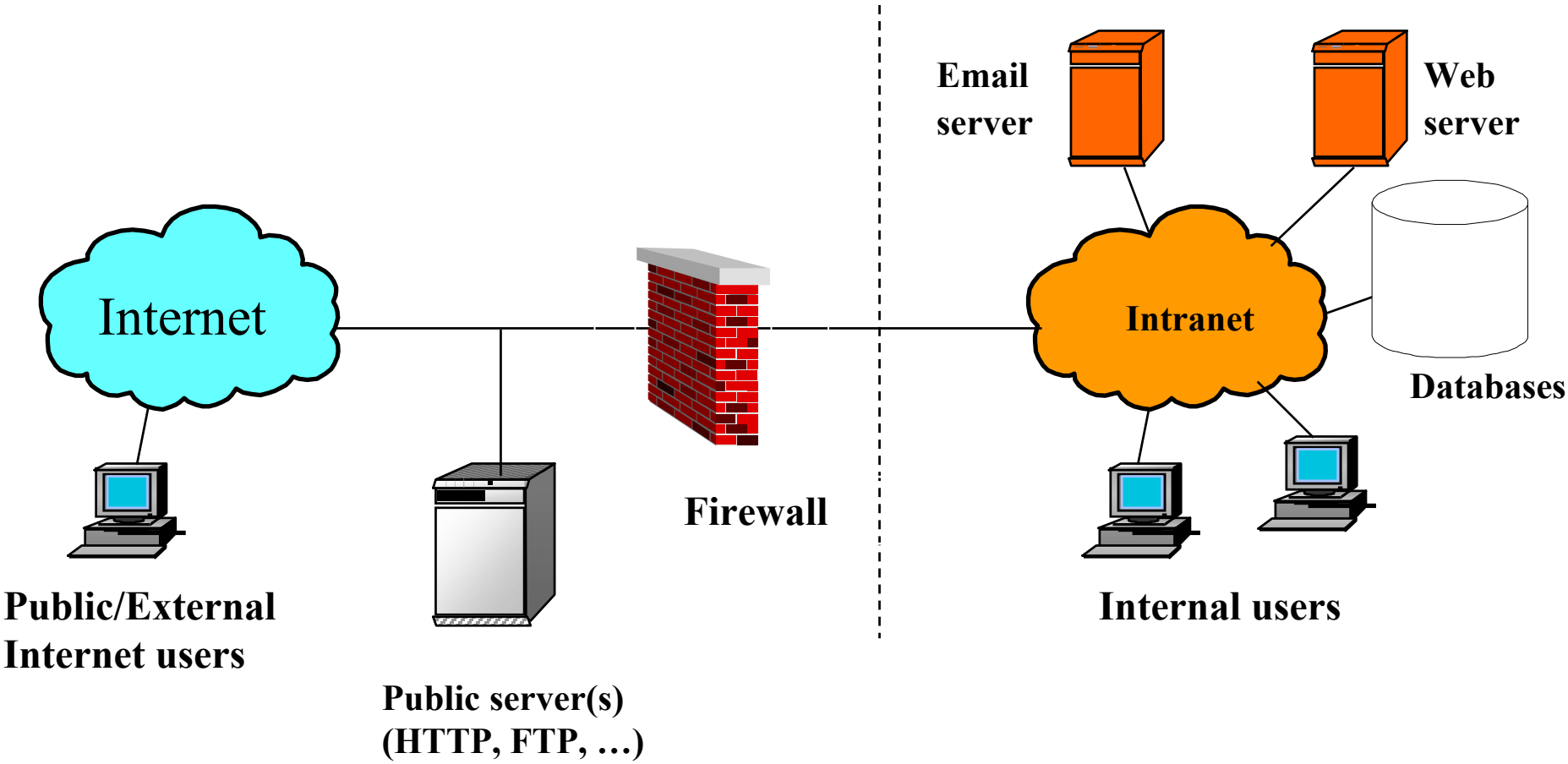
The Internet, Intranet, and Extranet

- **The Internet**
  - **A public and global communication network that provides connectivity via**
    - **a Local Area Network (LAN)**
    - **an Internet Service Provider (ISP)**
  - **Access to the Internet is not restricted to anyone.**
  - **Due to its vast scope and openness, the information is difficult to locate.**
  - **There is no centralized control of network and information.**

Intranet

- **An intranet is a corporate Local Area Network (LAN) and/or Wide Area Network (WAN)**
  - **Uses Internet technologies and protocols**
  - **Is secured behind company's firewalls**
- **They operate as private networks with limited access:**
  - **Only the users who are issued passwords and access codes are able to use them.**
  - **Intranets are limited to information pertinent to the company and contain exclusive and often proprietary and sensitive information.**
  - **Firewalls protect intranets from unauthorized outside access.**

Intranet (cont'd)



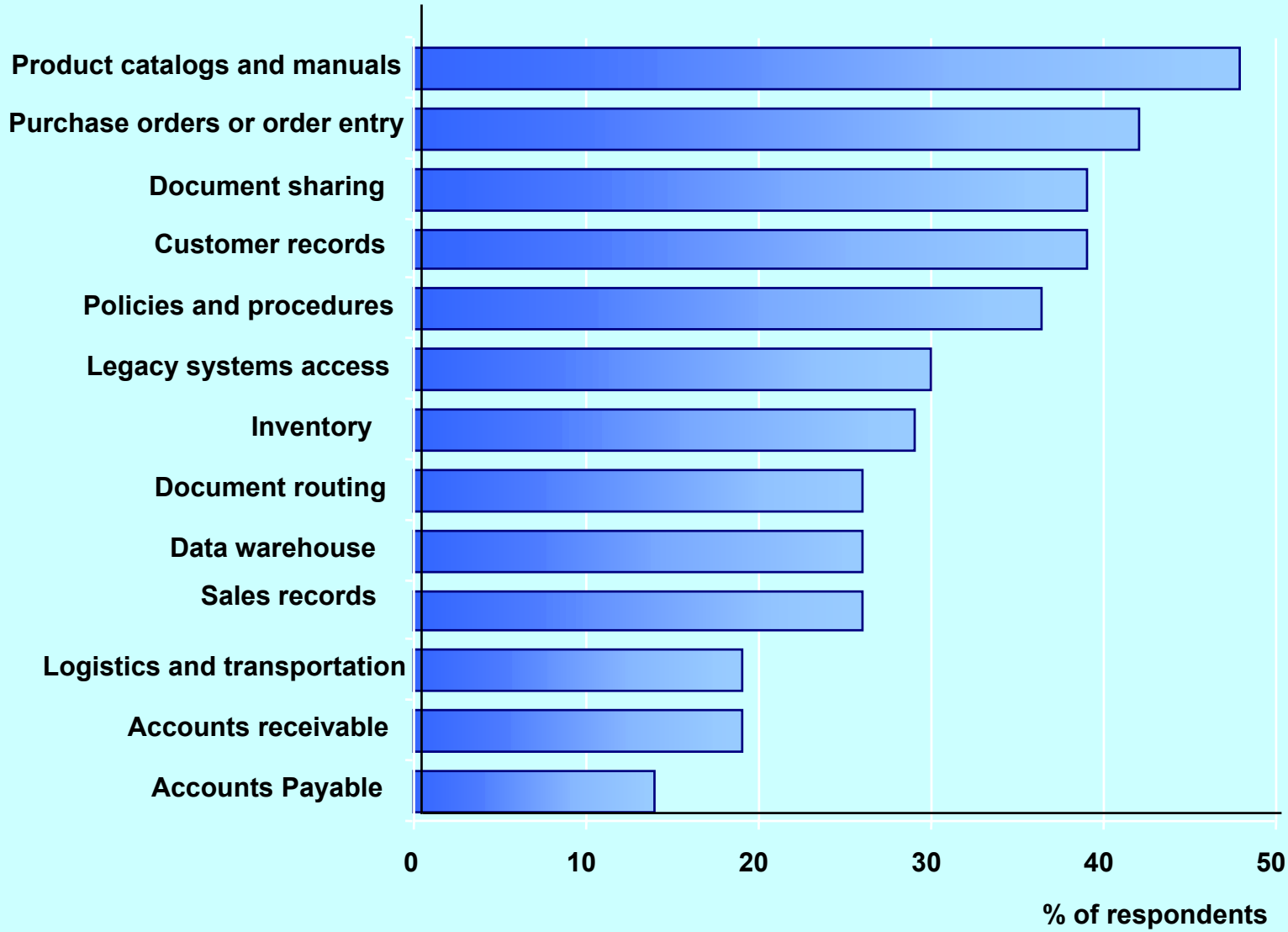
Functions of an Intranet

- ***Corporate/department/individual Web-pages***
- ***Interactive communication*: Chatting, audio and videoconferencing**
- ***Document distribution*: Web-based downloading of documents**
- ***Groupware*: E-mail and bulletin board**
- ***Telephony*: Intranets are the perfect conduit for computer-based telephony**
- ***Integration with electronic commerce*: Interface with Internet-based electronic sales and purchasing**

Intranet Applications

- ***Enhanced Knowledge Sharing*: Web pages can enhance knowledge sharing**
- ***Enhanced Group Decision and Business Processes*: Web-based groupware and workflow is becoming the standard intranet platform**
- ***Empowerment*: All information should be available to everyone with the ability to know and act independently**
- ***Virtual Organizations*: Web technology at participating departments/companies removes the barrier of incompatible communication technology**
- ***Software Distribution*: Using the intranet server as the application warehouse prevents many maintenance and support problems**
- ***Project Management*: Share reports and monitor projects' progress**

Categories of Intranet Application Purposes



S. Erfani, *Not to be reproduced without permission*

Intranet Deployment Requirements

- **Mission-critical intranet requirements:**
  - **Security: preventing potential attacks**
  - **Scalability: allowing for growth**
  - **Availability: minimum downtime**
- **Other requirements**
  - **Interoperability: allowing communication among various applications**
  - **Configurability: allowing commodity component substitutions**
  - **Compatibility: adherence to industry standards**
  - **Managability: allowing for device/element/network management**
  - **Reliability: allowing operational error immunity**
  - **Servicability: allowing for hot-swappable components and remote diagnostics**
  - **Stability: minimizes upgrade disruptions**

S. Erfani, *Not to be reproduced without permission*

Industry-Specific Intranet Solutions

- ***Financial Services*: Banking, brokerages and other financial services, insurance**
- ***Information Technology***
- ***Manufacturing*: Chemicals and oil, consumer goods, food and beverages, general manufacturing, and pharmaceuticals**
- ***Retailing***
- ***Services*: Construction and engineering, education, environmental, healthcare, media, entertainment, telecommunications, transportation, and utilities**

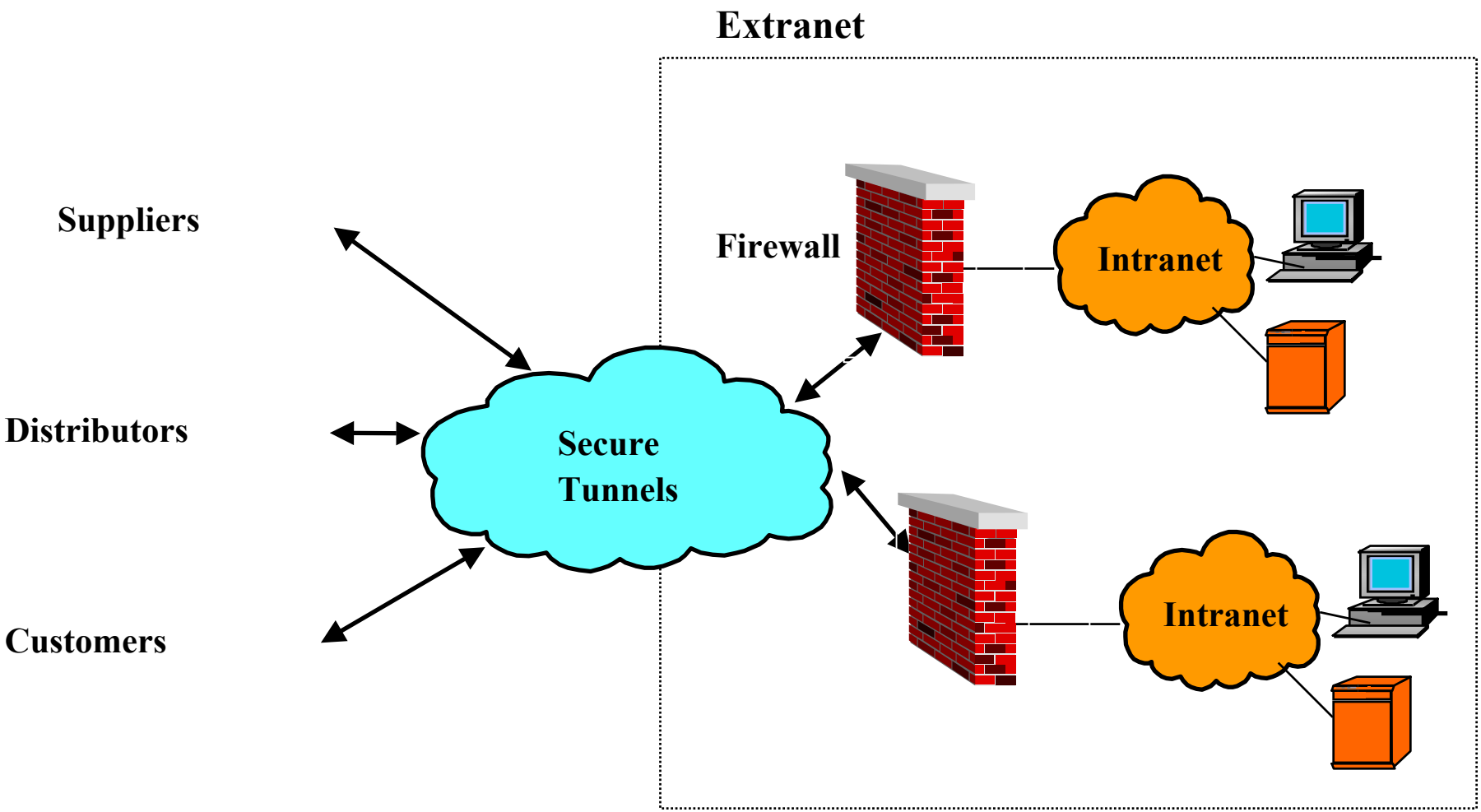
An Intranet Example

- **Federal Express**
  - **60 internal web sites allow communication worldwide between divisions and corporate headquarters on all issues of importance to the employees and customers**
  - **The package tracking system allows customers to contact FedEx and go into the intranet to find the status of a package that they have shipped or one that they are expecting**

Extranet

- **An extranet is an *extended intranet*: uses TCP/IP-based networks to link intranets in different locations**
- **Extranet transmissions are conducted over the Internet to save money.**
- **Security is improved by creating tunnels of secure data flow (VPNs).**
- **Extranets provide secure connectivity between a corporation's intranets and intranets of its**
  - **business partners**
  - **material suppliers**
  - **financial services, and**
  - **customers**

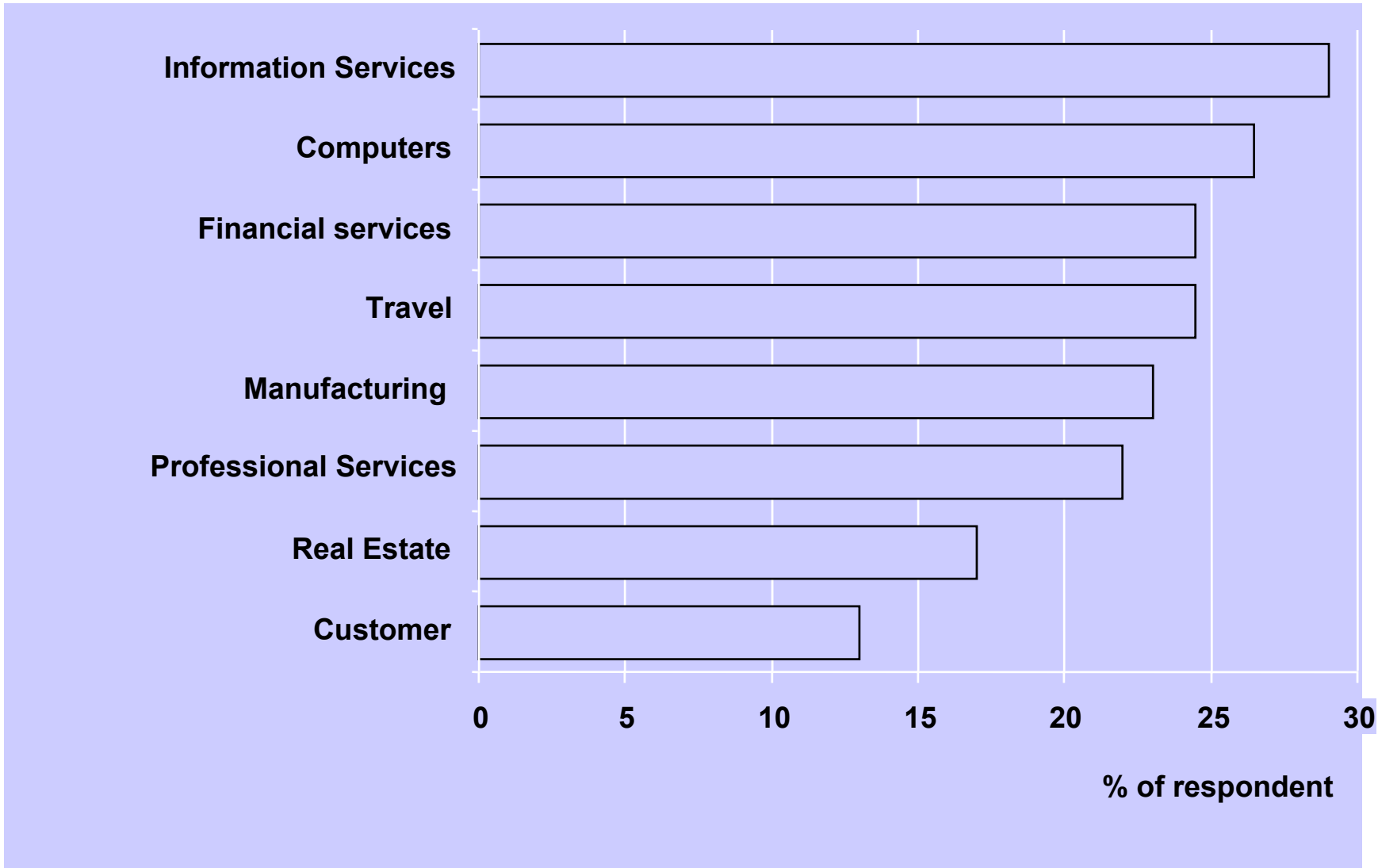
Extranet *(cont'd)*



Methods of Configuring Extranets

- **They can be implemented using a direct leased line with full control over it, linking all intranets**
- **A secure link can be created across the Internet, which can be used by the corporation as a VPN**

Industry-Specific Extranet Solutions



S. Erfani, *Not to be reproduced without permission*

An Extranet Example: Automotive Network Exchange (ANX)

- **ANX is the largest Extranet in the world.**
- **Companies in the automotive market share manufacturing data over ANX.**
- **It involves more than 10,000 companies.**
- **Includes CAD/CAM file transfers, Electronic Data Interchange (EDI), e-mail, and groupware.**

Benefits of ANX

- **ANX's EDI element alone will save $71 from the cost of designing and building each car.**
- **It provides an estimated savings of $1 billion a year for the Industry.**
- **Companies pay for fewer leased lines and satellite connections.**
- **Standardizing on one protocol suite (TCP/IP) reduces support costs.**
- **The time to turn around an order will be much shorter.**
- **The faster the parts come in, the faster the cars leave the assembly line, the larger the customer satisfaction and the manufacturer's profit.**

Other Extranet Examples

- **Reduced Product Development Cycle Time: Caterpillar, Inc.**
  - **Customers can use the extranet to retrieve and modify detailed order information while the vehicle remains on the assembly line**
- **Link the Worldwide Chains: Kinko's, Inc.**
  - **900 stores about 25,000 employees**
  - **Developed an extranet to offer Internet access and rental of PC computer time to its customers**
  - **Each store connects to the Internet with a 64-Kbps link**
- **Connect Auto dealers' Kiosk: General Motors Corp.**
  - **Kiosks in dealerships and shopping malls**
  - **Enable shoppers to purchase cars and trucks from anywhere**

Summary : Internet, Intranets, and Extranets

Network Type	*Typical Users*	*Type of Access*	*Information*
Internet	**Any individual with dial-up access or LAN**	**Unlimited, public; no restrictions**	**General, public and advertisement**
Intranet	**Authorized employees ONLY**	**Private and restricted**	**Specific, corporate and proprietary**
Extranet	**Authorized groups from collaborating companies**	**Private and outside authorized partners**	**Shared in authorized collaborating group**

S. Erfani, *Not to be reproduced without permission*

What Are the Threats to Intranets & Extranets?

- **As intranets and extranets increase and improve information sharing and connectivity, they make it easier for malicious intruders to attack security:**
  - **Denial of Service Attacks - achieved by flooding the target victims with enough volume (e.g., e-mail messages) so that the service cannot be used.**
  - **Packet Sniffing Attacks - achieved by using "packet sniffer programs" tapping a WAN wire.**
  - **IP Spoof Attacks - achieved by using the IP address of an unsuspecting victim.**
  - **Session Hijacking - achieved by a rogue device masquerading as a bona fide party in an ongoing communication.**
- **To reduce these risks, appropriate network access policies should be defined.**
- **Firewalls can be used to enforce network access policies.**

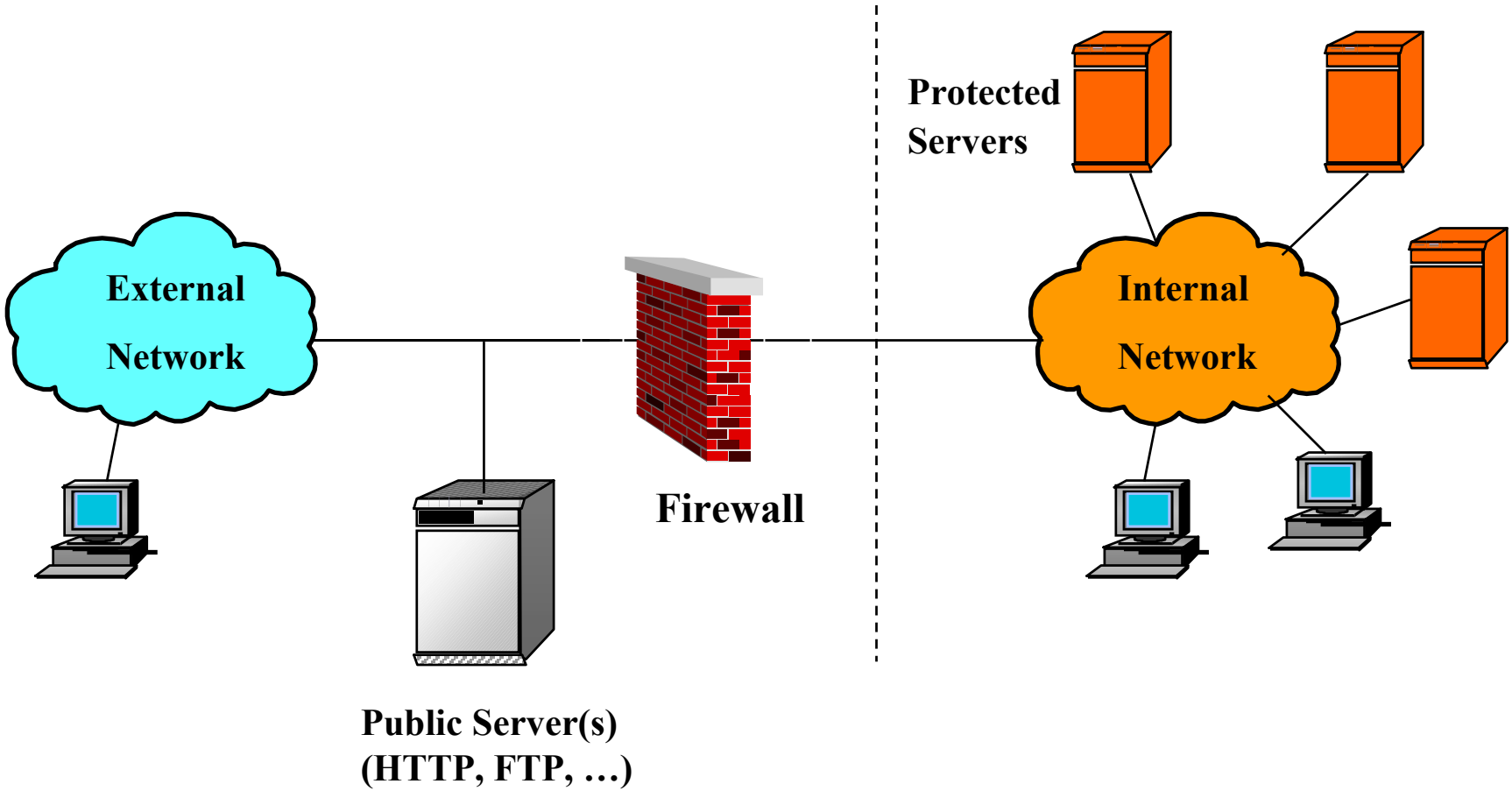
Firewall

- **A firewall is a network interconnection element that controls the traffic flowing between internal (protected) and external (public) networks.**
- **Can be implemented as a combination of hardware and software (almost 13% of information security budget*)**
- **Allows only external users with specific characteristics to access a protected network, and blocks others**
- **Used for one or more of the following reasons:**
  - **To prevent intruders from interfering with the operation of the protected network**
  - **To prevent intruders from modifying or deleting information stored within the protected network**
  - **To prevent intruders from obtaining private information stored within the protected network**
  - **To "segment" internal network**

***Network Security for Enterprises, The Yankee Group, Dec. 1996.**

Firewall (cont'd)

It is located at a gateway point between internal (private) and external (public) networks



Firewall Technologies

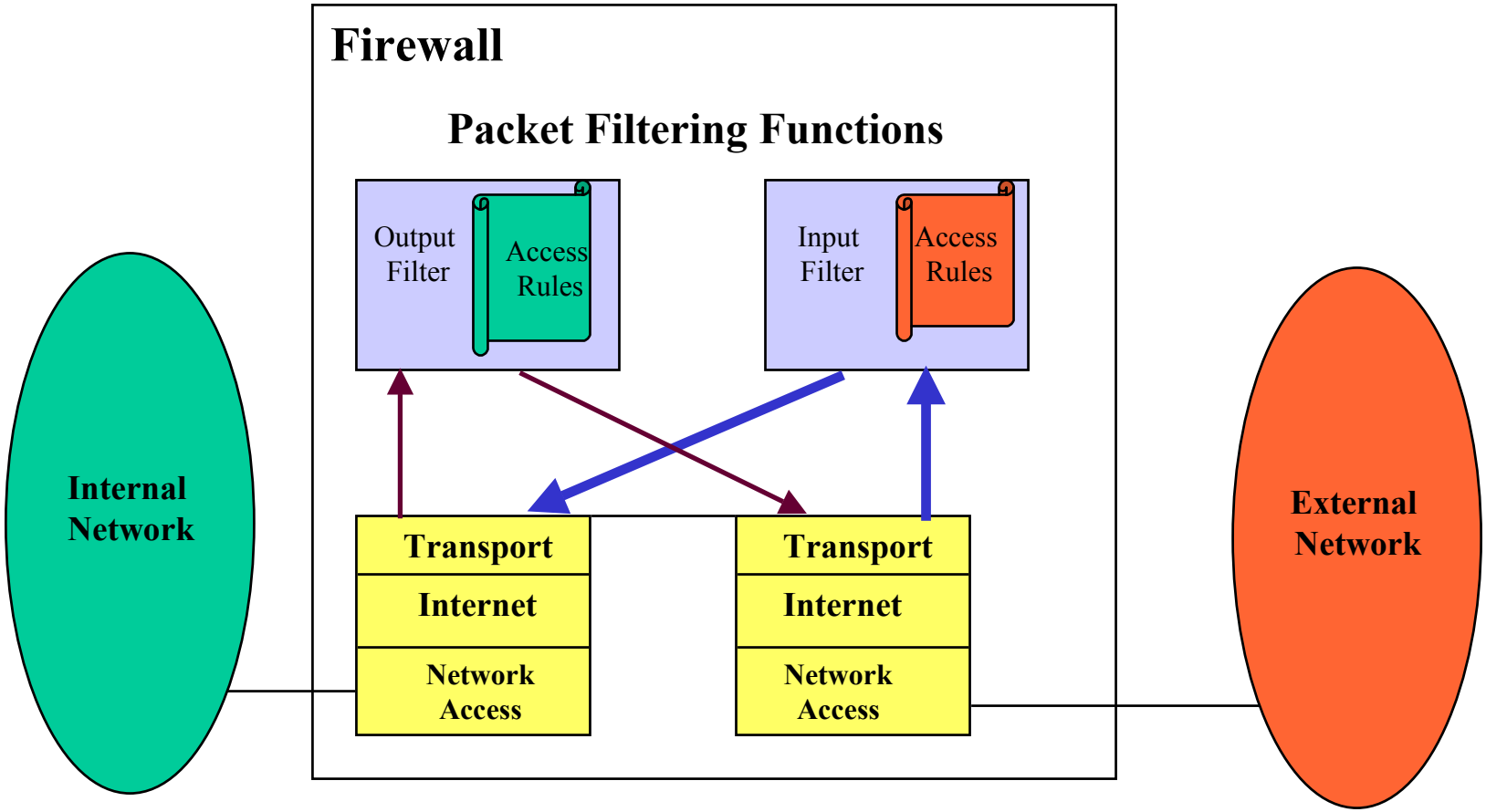
- **Three techniques are most commonly used in firewall products:**
  - **The simplest firewall consists of a *packet filter.***
  - **A more sophisticated firewall uses the *stateful packet filtering* technique.**
  - **The most sophisticated firewall consist of packet filters and *proxy servers*.**
- **Firewalls can be categorized according to the layers of the Internet protocol stack at which they operate.**
- **Firewalls may have encryption capability**

Packet Filtering Firewall

- **A *Packet Filtering Firewall* examines each packet header to determine whether to pass the packet to the internal network.**
- **This information used to police the traffic includes:**
  - **Source IP address and port number**
  - **Destination IP address and port number**
  - **Session protocol used (e.g., TCP, UDP, ICMP*, FTP)**
- **The firewall is not aware of the application information.**
- **Packet filtering is less processing intensive than other firewall technologies.**
- **Network access rules in packet filtering are *static.***

* Internet Control Message Protocol (ICMP), provides routing error handling, signaling, and connectivity testing.

Packet Filtering Firewall Functional Diagram

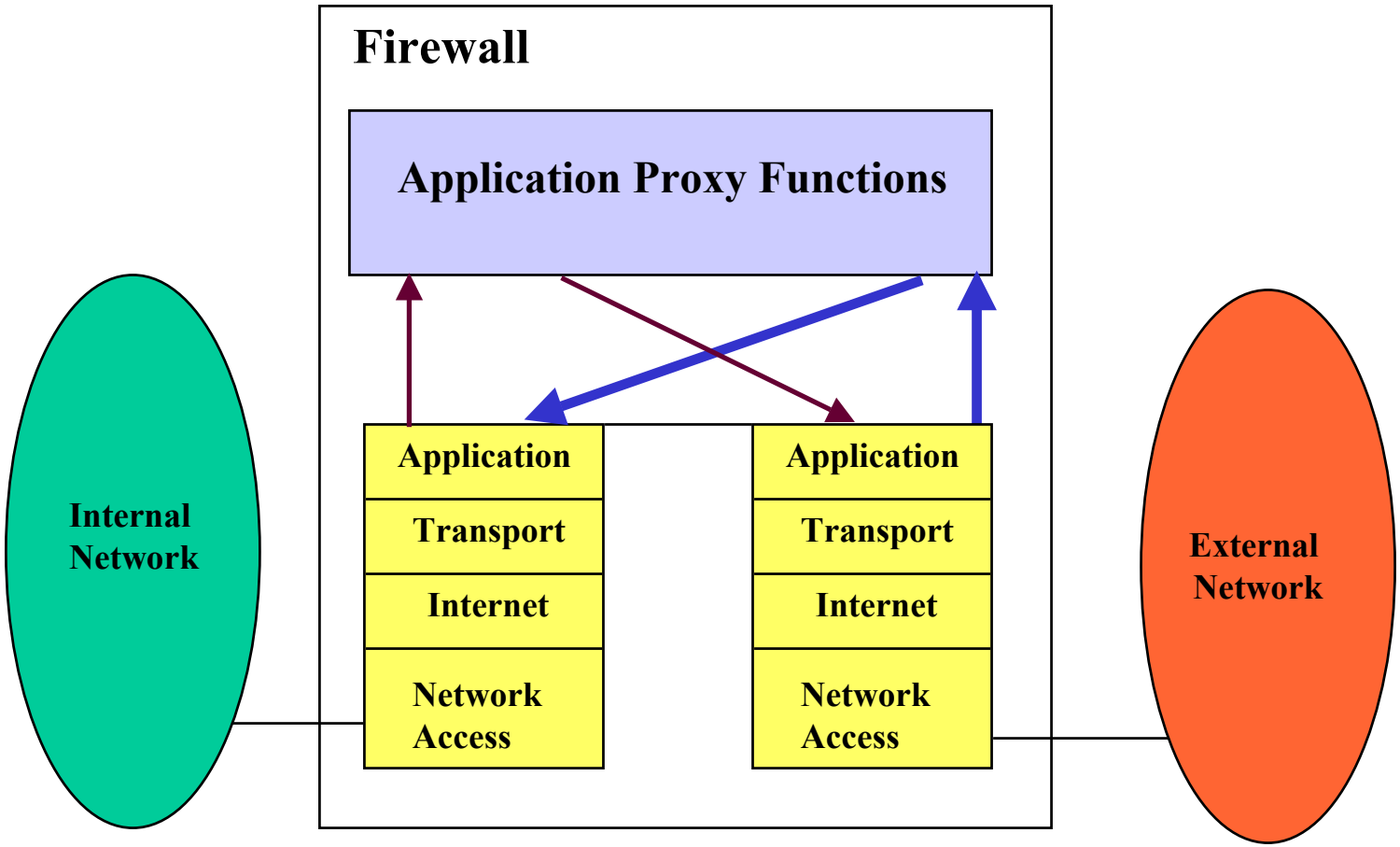


Proxy Server Firewalls

- **Traffic data is validated against service-specific, higher-layer access rules.**
- **Proxies work at the Transport Layer or at the Application Layer:**
  - **Proxies that provide Transport Layer relaying functions are called *circuit-level gateways*.**
  - **Proxies that provide Application Layer relaying functions are called *application gateways*.**

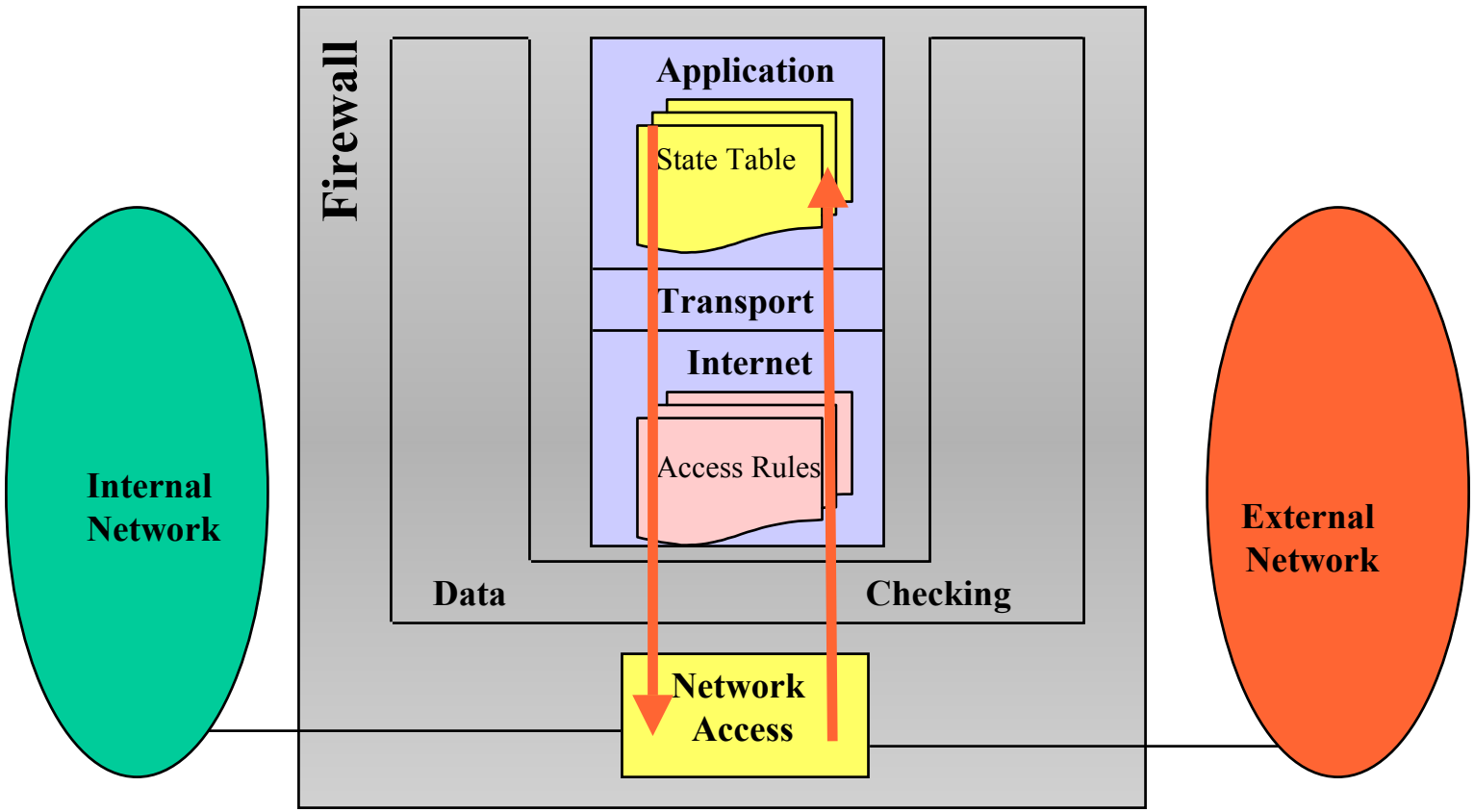
- **For each application to be supported, a corresponding proxy function needs to be running on the firewall.**
- **Application Gateway: Runs a suite of application-specific proxy functions through which all application data must pass**
  - **Filtering is done based on application data**
  - **Examples are e-mail, FTP, telnet, and Web servers.**

Application Gateway Functional Diagram



Stateful Packet Filtering

- Firewall *checks* the data at one or more layers.
- Incoming packets are checked in the context of previously received data by keeping track of session states.
- Firewall *dynamically adapts* its rules to changing network conditions.



Additional Firewall Functions

- **Password Protection:** Firewalls ensure that even if the passwords are compromised, the intruder has only restricted access to the rest of the network.
- **Access Control:** Firewalls can support the UDP-based Remote Authentication Dial-in User Service (RADIUS) protocol.

  (RADIUS is a database service that provides centralized Authentication, Authorization (i.e., access control), and Accounting (i.e., auditing) [AAA] services.)

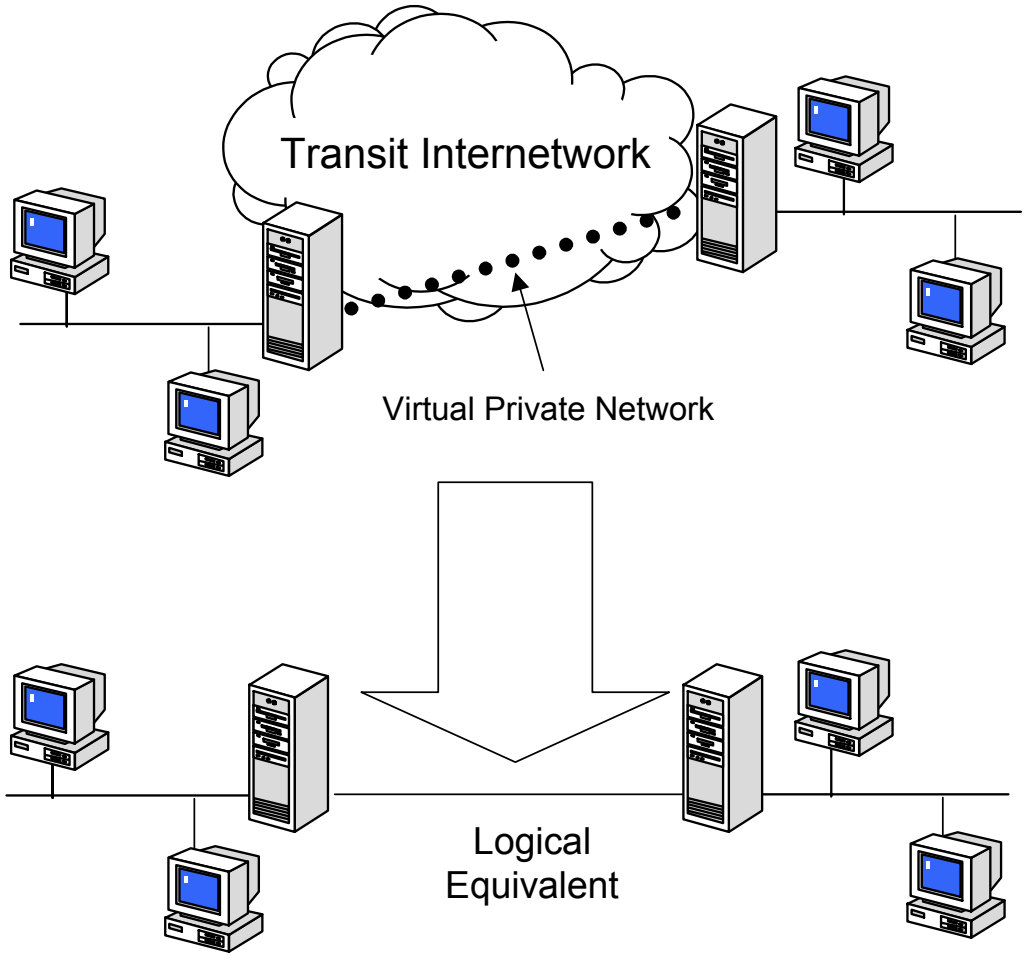
  Audit Trails: Firewalls have the capability to provide system event logging used to generate audit trails.
- **Tunneling:** Some firewalls have the capability to implement Virtual Private Network (VPN) functionality and *secure tunneling* over the Internet.
- **Network Address Translation (NAT):** Firewalls can hide the internal destination port numbers and IP address.

Virtual Private Networks (VPNs)

- **A VPN is a closed (private) network provided on shared infrastructure.**
- **A Virtual Private Network (VPN) connects the components and resources of a private network over a public network.**
- **VPNs can be provided over both packet-switched and circuit-switched public networks.**
- **The shared infrastructure can be the Internet, Frame Relay, or ATM network, or the Public Voice Networks (PSTN).**
- **Security is a major issue: VPN subscribers must have access to the VPN, but non-VPN subscribers must be blocked.**

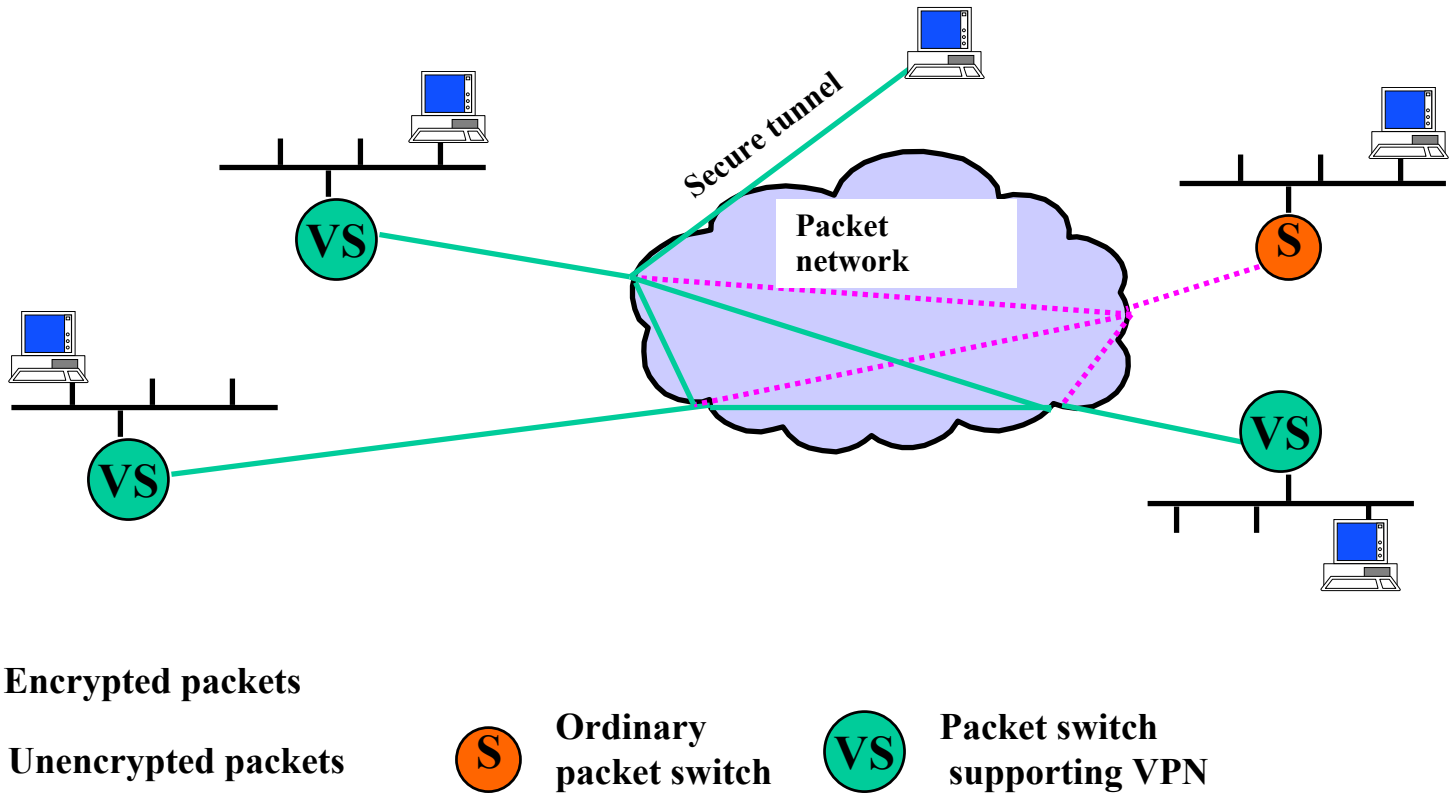
Objectives of VPN

- **From the user's perspective, the VPN is a point-to-point connection between the user's computer and a corporate server.**
- **VPNs allow tele-commuters, remote employees, or even branch offices to connect in a secure fashion.**



VPN over Packet-Switched Public Networks

- Some packet switches support VPN only.
- Some packet switches support public packets only.
- Some packet switches support both by using routing differentiation.
- Security must be provided for access to the VPN, and within the network.

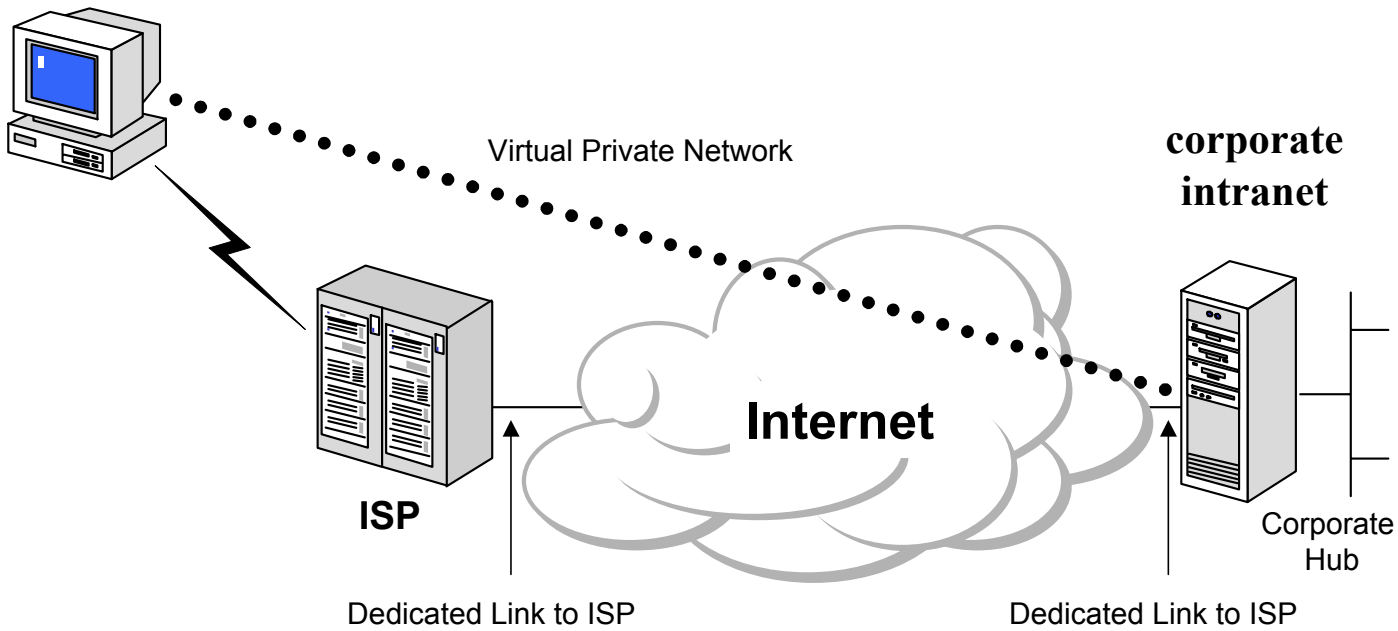


Internet-Based VPNs

- **Internet-based VPNs use the Internet as an inexpensive backbone.**
- **The Internet becomes part of a larger enterprise wide area network (WAN).**
- **A major issue is security:**
  - **VPN subscribers must have access to the VPN.**
  - **Non-VPN subscribers must be blocked from access to the VPN.**
  - **Confidentiality and integrity of the data transmitted over the Internet must be ensured.**
- ***Tunneling* is a method of using an internetwork infrastructure to transfer data from one network over another network.**

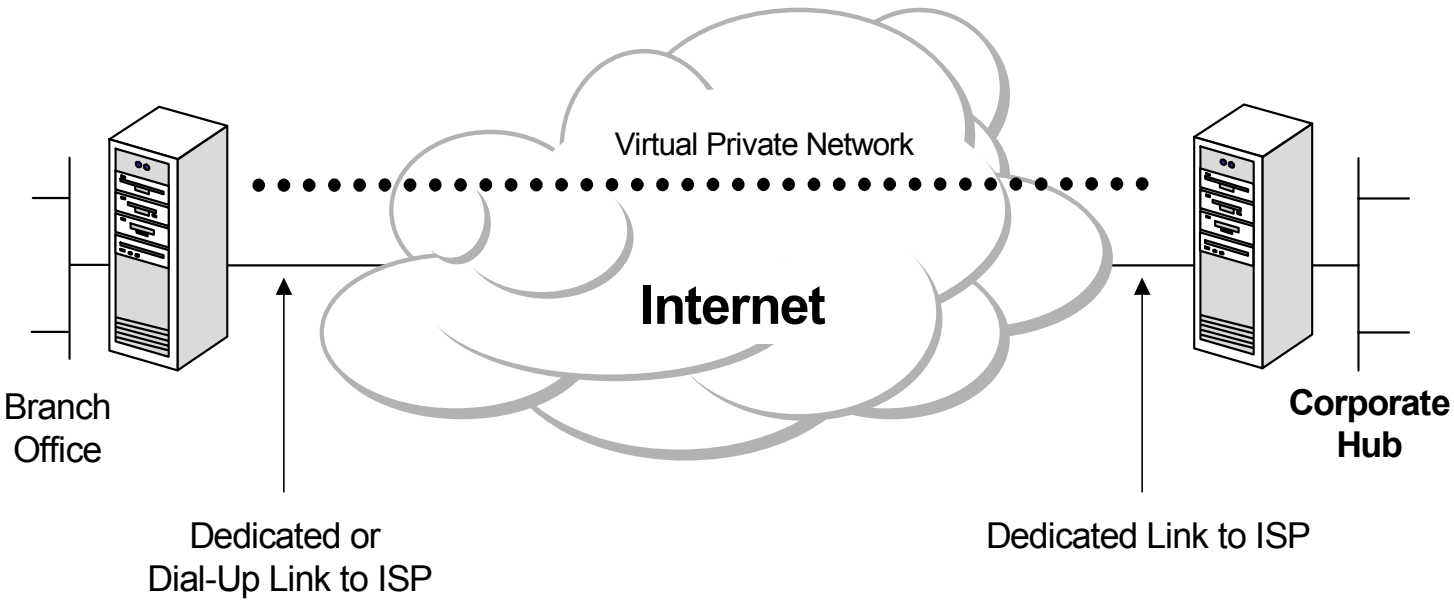
Common Uses of Internet-Based VPNs

- **Remote User Access over the Internet**
  - **To connect remote users to a corporate intranet using an Internet Service Provider (ISP) network.**
  - **The VPN software creates a secure connection between the dial-up user and the corporate intranet over the Internet.**



Common Uses of Internet-Based VPNs (cont'd)

- **Connecting networks over the Internet**
  - **Using a dial-up line to connect a branch office to a corporate LAN**



Factors Driving Demand for VPNs

- **Savings in infrastructure**
  - **For a hypothetical network consisting of 3 fully meshed sites in the US (LA, Boston, Houston) and a link to London, all at 64 Kb/s,**
  - **Leased lines:**
    - **Annual charges: $133,000**
    - **Installation charges: $2,700**
  - **Frame Relay VPN:**
    - **Annual charges: $90,000**
    - **Installation charges: $5,700**
    - **4 VPN encryption devices: $16,000**
  - **Internet VPN:**
    - **Annual charges: $38,400**
    - **4 VPN encryption devices: $16,000**
- **Savings in operation and administration**
  - **realized because the public network is administered by the VPN vendor.**

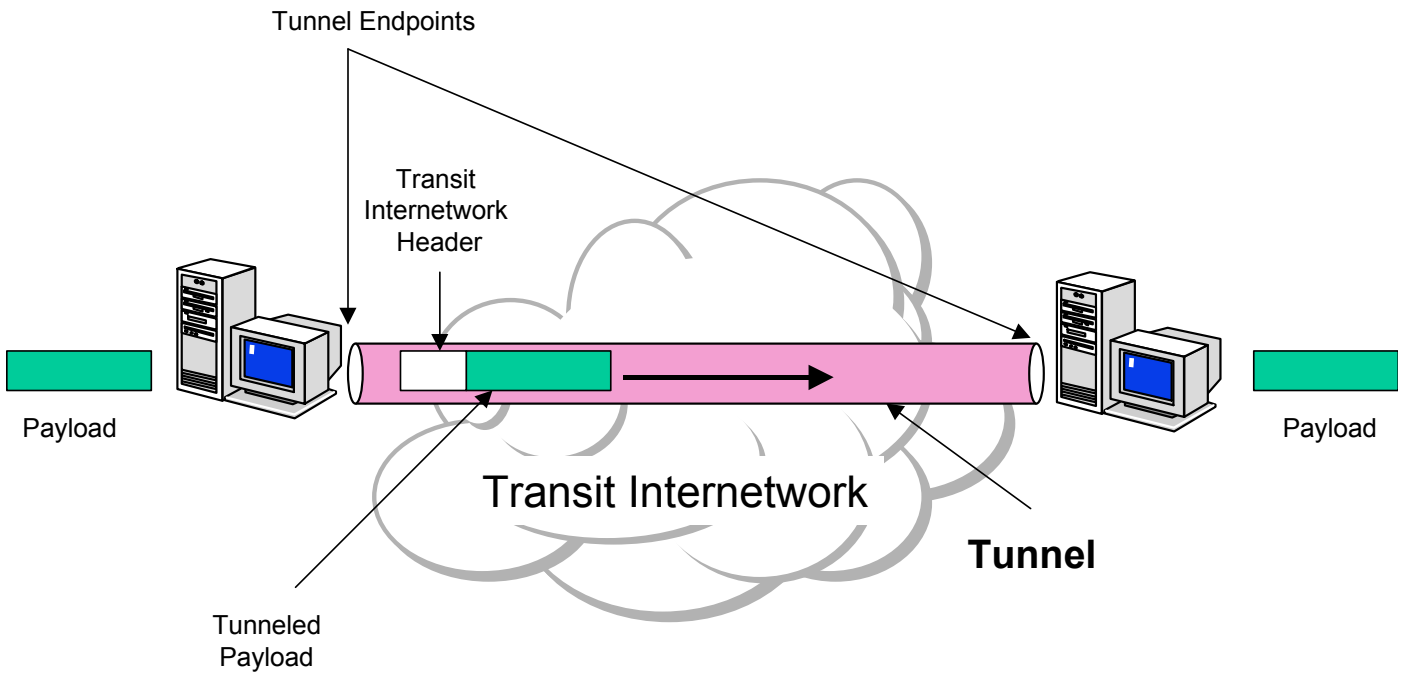
Requirements for Internet-Based VPNs

- **Security Requirements:**
  - ***User Authentication:*** **User's identity must be verified, and VPN access must be restricted to authorized users.**
  - ***Address Management and Privacy:*** **Clients' addresses on the private network must be kept private and managed securely.**
  - ***Data Integrity:*** **Data carried on the public network must be rendered unreadable to unauthorized clients.**

- **Security can be implemented in hardware or software.**
- **Security capabilities can be in firewalls or routers.**

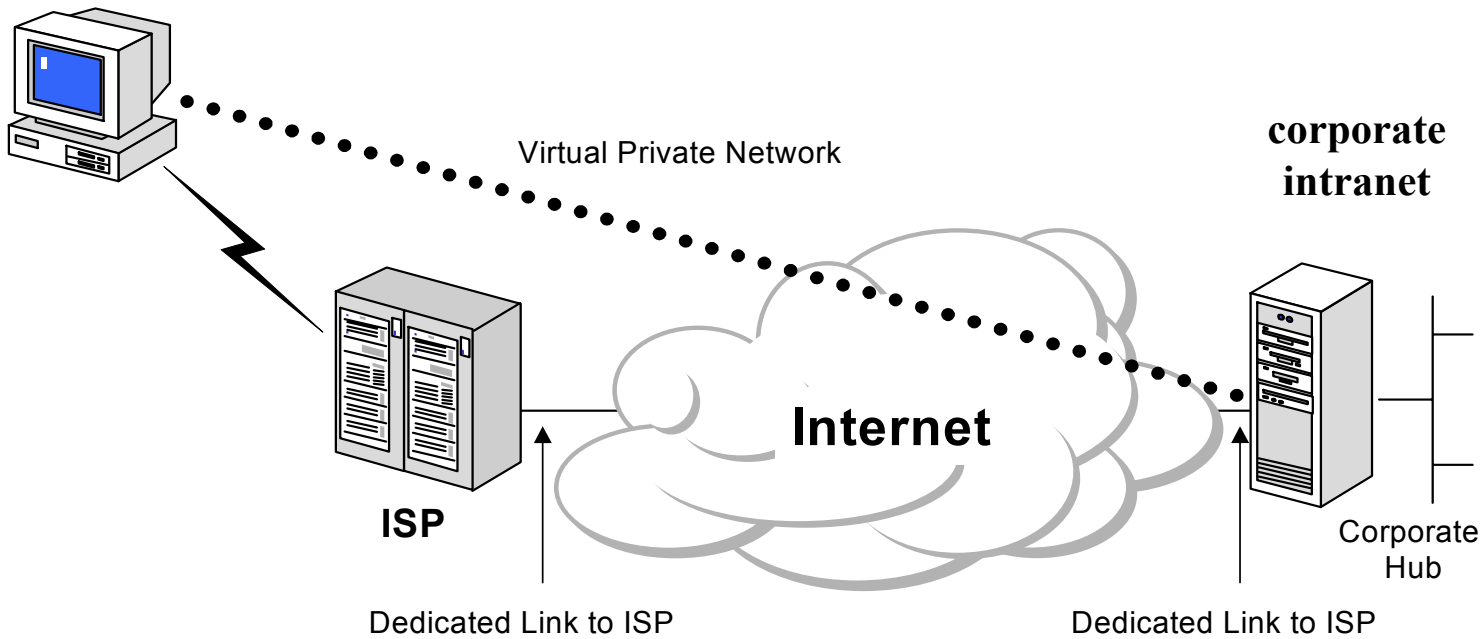
Tunneling

- ***Tunneling*: connecting a source network and a destination network of the same type over a network of a different type.**
  - **The tunneling protocol encapsulates each source packet in a frame to be carried through the intermediate (transit) internetwork.**
  - **Once the encapsulated frame reaches the destination network, the frame is un-encapsulated and forwarded to its final destination.**



Example: Secure Tunneling

To connect remote users securely to a corporate intranet using an Internet Service Provider (ISP) network



Tunneling Protocols

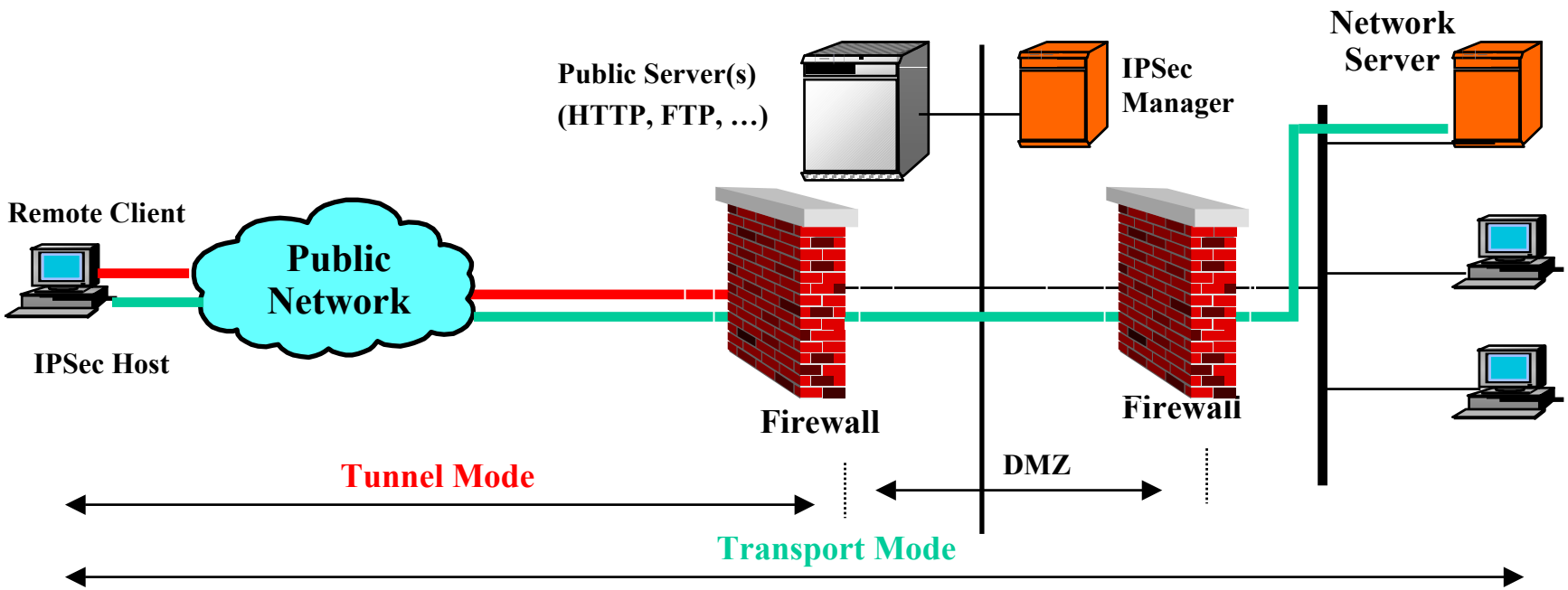
- **Point-to-Point Tunneling Protocol (PPTP), Microsoft's extension to Point-to-Point Protocol (PPP)**
- **Layer Two Forwarding (L2F, proposed by Cisco)**
- **IP Security (IPSec), an IETF standard: RFCs 1825, 1826, and 1827**
- **Generic Routing Encapsulation (GRE), IETF RFCs 1701 and 1702, established in 1994 as one of the pioneer tunneling protocols, used as the encapsulation technique for other tunneling protocols, such as PPTP**
- **Layer Two Tunneling Protocol (L2TP), another IETF standard for tunneling over IP, X.25, FR, or ATM networks**

IP Security (IPSec)

- **IPSec encompasses three functional areas:**
  - ***authentication:*** **It uses public-key digital certificates for authentication.**
  - ***confidentiality:*** **It encapsulates an IP datagram in a new encrypted packet.**
  - ***key management*****: is concerned with the secure exchange of keys.**
- **Characteristics of IPSec:**
  - **IPSec is below the transport layer (TCP, UDP), therefore transparent to applications and end users.**
  - **When implemented in a firewall router, it provides strong security to all traffic crossing the perimeter.**
  - **It allows a wide variety of authentication methods, e.g., MD5, SHA-1.**

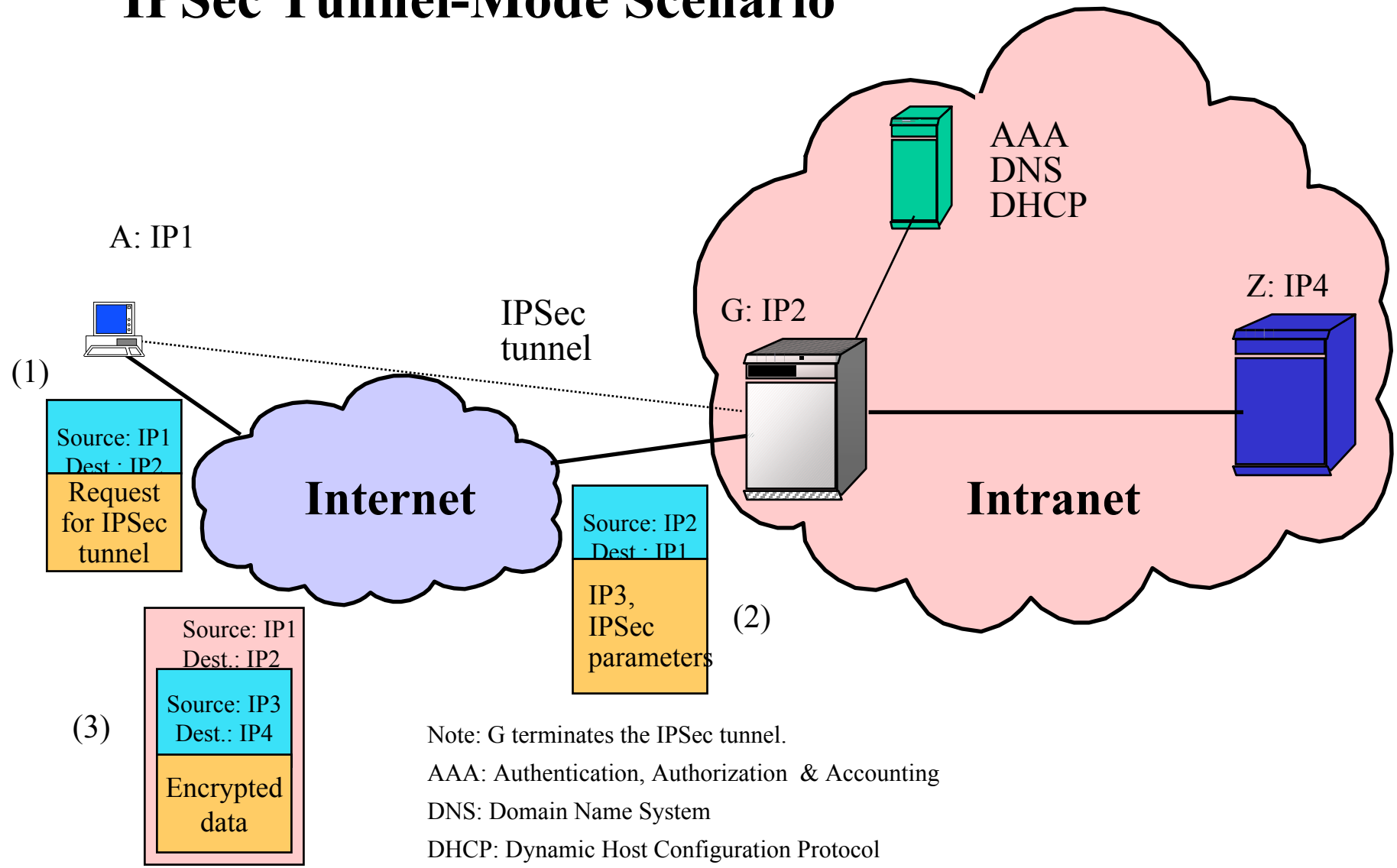
IPSec (cont'd)

- **Transport mode**
  - Encapsulates just the payload
  - Typically used for end-to-end communication between two hosts
- **Tunnel Mode**
  - Encapsulates the whole packet
  - Used when one or both ends of the connection is a security gateway, such as a firewall router.



DMZ: Demilitarized Zone

IPSec Tunnel-Mode Scenario



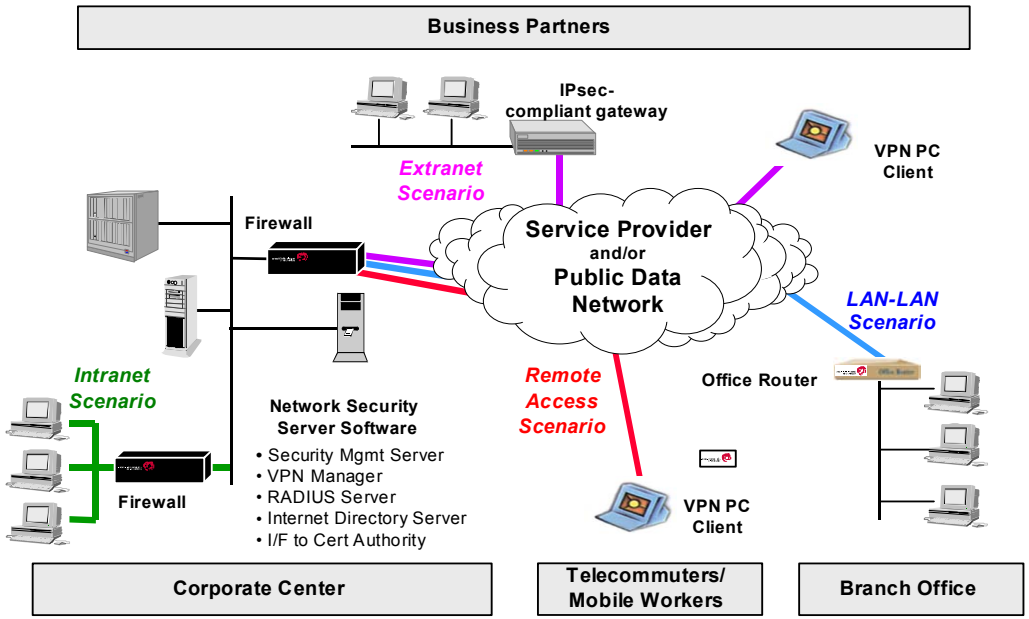
Note: G terminates the IPSec tunnel.

AAA: Authentication, Authorization & Accounting

DNS: Domain Name System

DHCP: Dynamic Host Configuration Protocol

Example of VPN Applications



Some Players and Vendors

- **ICSA certifies security products and coordinates several industry consortia for interoperability among product vendors (*http://www.trusecure.com*).**
- **AT&T, Level 3 Communications, MCI Worldcom, and Sprint Corp. are building VPN IP-over-ATM networks to carry voice, video, and data.**
- **VPN Gateways with Windows NT Operating System:**
  - **Intel *Lanover VPN* Gateway v6.7**
  - **Newbridge *Permit Gate 2500/4500* v2.1**
  - **CheckPoint Software *VPN-1Gateway/SecureServer* v4.1**
  - **F-Secure Corp. *F-Secure VPN+* v4.2**
- **Products with Proprietary Operating Systems:**
  - **Lucent *VPN Gateway 201*, V4.1**
  - **VPNet Technologies *VPNware VSU 1010 Gateway* VPNos 2.52**
  - **Axent Technologies, *Raptor Firewall with Integrated PowerVPN* v6.5**

* The VPN Source Page: <*http://www.internetwk.com/VPN/default.html*>